National Infrastructure Protection Center CyberNotes

Issue #2002-24 *December 2, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between November 6 and between November 29, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
acFree Proxy[1]	Windows NT	acFree Proxy 1.33 -beta7	A Cross-Site Scripting vulnerability exists when an error page is generated, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	acFreeProxy Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
acFTP[2]	Windows NT	acFTP 1.4	A vulnerability exists because users are allowed to authenticate without a valid password, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	acFTP Weak Authentication	Medium	Bug discussed in newsgroups and websites. Proof of Concept has been published.

[1] Securiteam, November 24, 2002.
[2] Securiteam, November 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alcatel[3]	Multiple	AOS 5.1.1	A vulnerability exists in the Alcatel OmniSwitch 7700 and 7800 models because an unintended backdoor is built into the system, which could let a remote malicious user obtain unauthorized access and full administrative control.	Fixes have been made available in versions 5.1.1.R02 and 5.1.1.R03 of AOS. Customers are advised to contact customer support for upgrades.	Alcatel AOS Default Telnet Server Remote Access CVE Name: CAN-2002-1272	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Allied Telesyn[4]	Multiple	AT-8024 1.3.1, Rapier 24	A remote Denial of Service vulnerability exists when a large stream of UDP data is submitted.	No workaround or patch available at time of publishing.	Allied Telesyn Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
America OnLine[5]	Multiple	Instant Messenger 5.0.2938	A vulnerability exists if an option is enabled that allows users to download files without a prompt, which could let a malicious user transfer an arbitrary file without consent.	No workaround or patch available at time of publishing.	AOL Instant Messenger Forced File Download	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
America OnLine[6]	Multiple	Instant Messenger 5.1.3036	A buffer overflow vulnerability exists when viewing the information about a screen name containing 88 characters or longer, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Instant Messenger Screen Name Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
BizDesign[7]	Windows, Unix	ImageFolio 2.23, 2.24, 2.26, 2.27, 3.0.1	A Cross-Site Scripting vulnerability exists in various CGI scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ImageFolio Cross-Site Scripting CVE Name: CAN-2002-1334	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Calisto Calisto[8]	Unix	Internet Talker 0.4	A remote Denial of Service vulnerability exists when an excessive amount of data is submitted to the Calisto daemon.	No workaround or patch available at time of publishing.	Internet Talker Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[3] CERT Advisory CA-2002-32, November 21, 2002.
[4] Bugtraq, November 20, 2002.
[5] Bugtraq, November 25, 2002.
[6] Bugtraq, November 17, 2002.
[7] SecurityTracker Alert ID, 1005681, November 22, 2002.
[8] Security Freaks Advisory, SFAD02-002, November 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[9]	Multiple	PIX Firewall 5.0, 5.1, 5.1 (4.206), 5.1.4, 5.2, 5.2 (2), 5.2 (3.210), 5.2 (5), (6), (7), 6.0, 6.0 (1), (2), 6.0.3, 6.1, 6.1 (2), 6.1.3, 6.2, 6.2 (1), 6.2.1	A buffer overflow vulnerability exists in the HTTP RADIUS/TACACS+ proxy component when a specially malformed request is processed, which could let a malicious user cause a Denial of Service and possible execute arbitrary code.	Upgrade available at: http://www.cisco.com/pcgi-bin/tablebuild.pl/pix	PIX TACACS+/ RADIUS HTTP Proxy Buffer Overrun	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Cisco Systems[10]	Multiple	PIX Firewall 6.0, 6.0 (1), 6.0 (2), 6.0.3, 6.1, 6.1 (2), 6.1.3	A vulnerability exists in the way VPN sessions are handled due to insecure handling through the Internet Security Authentication Key Management Protocol (ISAKMP) Security Associations (SAs) implemented, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://www.cisco.com/pcgi-bin/tablebuild.pl/pix	PIX Firewall VPN Session	Medium	Bug discussed in newsgroups and websites.
Curtis Specialty Consulting[11]	Windows 2000	IISPop 1.161, 1.181	A remote Denial of Service vulnerability exists when an unusually large amount of data is submitted on TCP port 110. Arbitrary code execution may be possible.	No workaround or patch available at time of publishing.	IISPop Remote Denial of Service	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Double Precision Incorporated[12, 13]	Unix	Courier MTA 0.37.3, 0.40	A vulnerability exists because privileges are not dropped fast enough upon startup, which could let a malicious user obtain sensitive information.	**Debian:** http://security.debian.org/pool/updates/main/c/courier	Courier SqWebMail File Disclosure	Medium	Bug discussed in newsgroups and websites.
Ehud Gavron[14]	Unix	TrACES route 6.0, 6.1, 6.1.1	Two buffer overflow vulnerabilities exist due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.suse.com/pub/suse/	Traceroute-Nanog Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Francisco Burzi[15]	Multiple	PHP-Nuke 5.0, 5.0.1, 5.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0, 6.5 BETA 1	Several Cross-Site Scripting vulnerabilities exist due to insufficient filtering, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PHP-Nuke Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

[9] Cisco Security Advisory, 20021120, November 20, 2002.
[10] Cisco Security Advisory, 20021120, November 20, 2002.
[11] Bugtraq, November 14, 2002.
[12] Debian Security Advisory, DSA 197-1, November 15, 2002.
[13] Gentoo Linux Security Announcement, 200211-005, November 19, 2002.
[14] SuSE Security Announcement, SuSE-SA:2002:043, November 12, 2002.
[15] Bugtraq, November 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeNews[16]	Unix	FreeNews 2.1	A vulnerability exits because it is possible to place commands in include files, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	FreeNews Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.
Ghost View[17] ***Patches are released[18, 19, 20, 21, 22, 23, 24, 25]*** ***More patches released 26, 27***	**Unix**	**GhostView 1.3, 1.4, 1.4.1, 1.5, gv 2.7 b1-b5, 2.7.6, 2.9.4, 3.0.0, 3.0.4, 3.1.4, 3.1.6, 3.2.4, 3.4.2, 3.4.3, 3.4.12, 3.5.2, 3.5.3, 3.5.8**	**A buffer overflow vulnerability exists in the sscanf() function when a malformed postscript or Adobe pdf file is sent, which could let a malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.** ***Debian:*** **http://security.debian.org/pool/updates/main/g/gnome-gv/** http://security.debian.org/pool/updates/main/k/kdegraphics ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com/** ***KDE:*** **ftp://ftp.kde.org/pub/kde/security_patches/post-2.2.2-kdegraphics-kghostview.diff** **SCO:** **ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/Workstation/CSSA-2002-053.0/RPMS/gv-3.5.8-10.i386.rpm** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/**	**GhostView Buffer Overflow** **CVE Name: CAN-2002-0838**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Gordano[28]	Windows NT 4.0/2000, XP	NTMail 8.0	A vulnerability exists in the JUCE filter due to insufficient filtering of some e-mail, which could let a remote malicious user send e-mail that will bypass the SPAM keyword filter.	Hotfix available at: ftp://ftp.gordano.com/gms/hotfixes/h20021119/intel/smtp_h20021119.zip	NTMail JUCE E-mail Filter	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[16] SecurityFocus, November 26, 2002.
[17] iDEFENSE Security Advisory, 09.26.2002, September 26, 2002.
[18] Gentoo Linux Security Announcement, 200210-003, October 17, 2002.
[19] Debian Security Advisory, DSA 176-1, October 16, 2002.
[20] Debian Security Advisory, DSA 179-1, October 18, 2002.
[21] Debian Security Advisory, DSA 182-1, October 28, 2002.
[22] Mandrake Linux Security Update Advisory, MDKSA-2002:069, October 22, 2002.
[23] Mandrake Linux Security Update Advisory, MDKSA-2002:071, October 24, 2002.
[24] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:212-06, October 4, 2002.
[25] KDE Security Advisory, October 9, 2002.
[26] Conectiva Linux Security Announcement, CLA-2002:542, November 6, 2002.
[27] SCO Security Advisory, CSSA-2002-053.0, November 22, 2002.
[28] SecurityTracker Alert ID, 1005650, November 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hughes Technologies[29] ***Patch now available*** [30]	**Unix**	**LibHTTPD 1.2**	**A buffer overflow vulnerability exists when an POST request is submitted that is of excessive length, which could let a malicious user execute arbitrary code with super user privileges.**	***Upgrade available at:*** **http://www.hughes.com.au/products/libhttpd/libhttpd-1.3.tar.gz**	**LibHTTPD POST Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
IBM[31]	Unix	AIX 4.3.3, 5.1	A Denial of Service vulnerability exists when the Selective Acknowledgements network option is implemented if the number of TCP packet retransmissions submitted exceed the level specified by the system.	Upgrades available at: IBM APAR IY30696: http://techsupport.services.ibm.com/support/rs6000.support/fixsearch?fixdb=aix4&srchtype=apar&query=IY30696 IBM APAR IY30975: http://techsupport.services.ibm.com/server/aix.fixdist51?fixes=IY30975&whichFix=APAR	AIX Selective ACK Denial of Service	Low	Bug discussed in newsgroups and websites.
IBM[32]	Multiple	HTTP Server 1.0	A vulnerability exists when a non-existent .jsp file is requested, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	IBM HTTP Server Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Jelsoft Enterprises[33]	Unix	VBulletin 2.0 rc 2&3, 2.0.3, 2.2.0-2.2.9	A Cross-Site Scripting vulnerability exists due to improper filtering of HTML tags from URI parameters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	VBulletin Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Jelsoft Enterprises[34]	Unix	vBulletin 2.0-2.0.2, 2.2.0- 2.2.9 can	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user supplied values, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	VBulletin members2.php Cross Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
KDE[35]	Unix	KDE 2.1-2.2.2, 3.0-3.0.4	A vulnerability exists in the KIO subsystem rlogin and telnet protocols, which could let a remote malicious user execute arbitrary commands.	**KDE:** http://download.kde.org/stable/3.0.5/	KDE KIO Subsystem Network Protocol Implementation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[29] INetCop Security Advisory, 2002-0x82-003, November 13, 2002.
[30] Hughes Technology, November 25, 2002.
[31] SecurityTracker Alert ID, 1005604, November 12, 2002.
[32] Bugtraq, November 13, 2002.
[33] Securiteam, November 21, 2002.
[34] SecurityFocus, November 25, 2002.
[35] KDE Security Advisory, November 11, 2002

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KeyFocus Ltd.[36]	Windows 98/ME/ 2000, XP	KF Web Server 1.0.8	A Directory Traversal vulnerability exists due to the inability to properly handle filenames that contain consecutive dot characters, which could let a remote malicious user obtain sensitive information.	This issue has been addressed in KF Web Server version 2.0.0 beta and will also reportedly be fixed in the next stable release.	KF Web Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
LBL[37]	Unix	tcpdump 3.4 a6, 3.4, 3.5, 3.5.2, 3.6.2	A vulnerability exists due to a miscalculation in the use of the sizeof operator, which could let a malicious user cause a Denial of Service or execution of arbitrary code.	**SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/	TCPDump Memory Corruption	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Lib CGI[38]	Unix	Lib CGI 0.1	A buffer overflow vulnerability exists in the development library due to improper bounds checking in an include file, which could let a remote malicious user obtain unauthorized access with privileges of the web server process.	No workaround or patch available at time of publishing.	Lib CGI Include Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

Linksys Group, Inc.[39]	Multiple	BEFW11S4 1.4.2 .7, 4 1.4.3;
		EtherFast BEFSR11 Router 1.41, 1.42.3, 1.42.7, 1.43;
		BEFSR41 Router 1.41, 1.42.3, 1.42.7, 1.43;
		BEFSRU31 Router 1.41, 1.42.3, 1.42.7, 1.43
			A vulnerability exists during the negotiation stage due to a failure to handle XML-related data transmitted by clients during initialization, which could let a malicious user bypass authentication and obtain administrative access.	Linksys has released firmware version 1.43.3 that resolves this issue available at: http://www.linksys.com/download/	Linksys Router Unauthorized Management Access	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[36] Bugtraq, November 13, 2002.
[37] SCO Security Advisory, CSSA-2002-050.0, November 20, 2002.
[38] INetCop Security Advisory, 2002-0x82-007, November 27, 2002.
[39] Securiteam. November 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Linksys Group Inc.[40]	Multiple	BEFN2PS4 1.42.7, BEFSX41 1.42.7, BEFVP41 1.42.7, BEFW11S 4 1.4.2.7, 1.4.3, EtherFast BEFSR11 Router 1.42.7, 1.43, BEFSR41 Router 1.42.7, 1.43, BEFSR81 Router 2.42.7, BEFSRU31 Router 1.42.7, 1.43, HPRO200 1.42.7	A buffer overflow vulnerability exists when an overly long string is submitted for the password field, which could let a local/remote malicious user cause a Denial of Service.	Upgrade available at: http://www.linksys.com/download/	Multiple Linksys Devices Password Field Buffer Overflow CVE Name: CAN-2002-1312	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Lone-runner[41]	Windows, Unix	Zeroo HTTP Server 1.5	A buffer overflow vulnerability exists due insufficient bounds checking on some requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Zeroo HTTP Server Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Macro-media[42]	Windows NT	Flash 6.0.47 .0	A buffer overflow vulnerability exists in the SWRemote parameter used in Macromedia Flash objects, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Flash SWRemote Heap Corruption	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mail Enable[43]	Windows NT	MailEnable 1.5 015-1.5 018	A buffer overflow vulnerability exists in the POP3 server due to insufficient bounds checking of the USER login field, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MailEnable E-mail Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[40] iDEFENSE Security Advisory, 11.19.02a, November 19, 2002.
[41] INetCop Security Advisory, 2002-0x82-004, November 16, 2002.
[42] Bugtraq, November 18, 2002.
[43] Securiteam, November 21, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mc Murtrey/ Whitaker & Associates[44]	Windows 98/ME/NT 4.0/2000	Cart32 2.5a, 2.6, 3.0, 3.1, 3.5a Build 710, 3.5a, 3.5 Build 619, 3.5, 4.4	A vulnerability exists due to insufficient validation of hidden form field information, which could let a malicious user manipulate sensitive information.	No workaround or patch available at time of publishing.	Cart32 Insufficient Validation Hidden Form Field	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
MHonArc[45]	Unix	MHonArc 2.4.4, 2.5.2, 2.5.13	A Cross-Site Scripting vulnerability exists when configured to display all header lines on the web, which could let a malicious user execute arbitrary HTML and script code.	**Debian:** http://security.debian.org/pool/updates/main/m/mhonarc/	MHonArc Mail Cross-Site Scripting CVE Name: CAN-2002-1307	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[46]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.0 for Windows 95/98/ 2000, 5.0 for Windows NT 4.0, 5.0.1, 5.0.1 SP1&2, 5.0.1 for Windows 95/98/ 2000, 5.0.1 for Windows NT 4.0, 5.5, 5.5 SP1&2, Internet Explorer 6.0, 6.0SP1	A vulnerability exists in the dialogArguments object when an IFRAME in a dialog changes its location or Zone, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer IFRAME dialog Arguments	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[47]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1; MDAC 2.1, 2.5, 2.6	A buffer overflow vulnerability exists in the Remote Data Services (RDS) Data Stub due to an unchecked buffer, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-065.asp	Microsoft Data Access Components RDS Buffer Overflow CVE Name: CAN-2002-1142	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[44] WhiteHat Security Advisory 1004, November 11, 2002.
[45] Debian Security Advisory, DSA 199-1, November 19, 2002.
[46] Bugtraq, November 9, 2002.
[47] Microsoft Security Bulletin, MS02-065 V1.1, November 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[48]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in MSIE due to improper checking of PNG graphic file parameters, which could let a remote malicious user cause a Denial of Service; an information disclosure vulnerability exists due to the way encoded characters in a URL are handled, which could let a malicious user obtain sensitive information; a vulnerability exists due to improper handling of the OBJECT tag, which could let a remote malicious user obtain sensitive information; and three vulnerabilities exists due to incomplete security checks when particular programming techniques are used, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-066.asp	Multiple Internet Explorer Vulnerabilities CVE Names: CAN-2002-1185, CAN-2002-1186, CAN-2002-1187, CAN-2002-1188, CAN-2002-1254, CAN-2002-1217	Low/ Medium/ **High** **Low if a DoS; Medium if sensitive informa-tion can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Microsoft[49]	Multiple	Virtual Machine 3802 Series, 3805 Series	A vulnerability exists because an applet that is constructed at the bytecode-level may be able to perform some illegal operations, which could let a malicious user bypass security constraints and execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft Java Virtual Machine Bytecode Verifier	**High**	Bug discussed in newsgroups and websites.

[48] Microsoft Security Bulletin, MS02-066 V1.1, November 25, 2002.
[49] Bugtraq, November 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[50] ***Microsoft updates patch***[51]	**Windows 98/ME/NT 4.0/2000, XP, Mac OS 8.1 to 9.x, MacOS X**	**Windows 98, ME, NT 4.0, NT 4.0 Terminal Server Edition, 2000, XP, Office for Mac, Internet Explorer for Mac, Outlook Express for Mac**	**A vulnerability exists because due to the way the Basic Constraints field validates a digital certificate, which could let a malicious user act as a Certificate Authority and create subordinate certificates with any desired information, set up a web site that poses as a different web site, and "proving" its identity by establishing an SSL session as the legitimate web site, send e-mails signed using a digital certificate that purportedly belongs to a different user, spoof certificate-based authentication systems to gain entry as a highly privileged user, or digitally sign malware using an Authenticode certificate that claims to have been issued to a company users might trust.** ***The newly discovered vulnerability is closely related to the one discussed in the original version of the bulletin and, like that vulnerability, involves a flaw in the way certificate validation is performed. However, this vulnerability could enable a malicious user to obtain control over a user's system***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-050.asp** ***An updated version of the patch has been released that not only eliminates the original vulnerability but also eliminates a newly discovered variant of the original vulnerability.***	**Microsoft Certificate Validation** **CVE Name: CAN-2002-0862**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** **Vulnerability has appeared in the press and other public media.**
Mozilla[52]	Multiple	Bugzilla 2.10, 2.12, 2.14, 2.14.1-2.14.4, 2.16, 2.16.1, 2.17	A Cross-Site Scripting vulnerability exists due to improper sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. *Note: This vulnerability only affects users who have the 'quips' feature enabled.*	Information for upgrading available at: http://bugzilla.mozilla.org/show_bug.cgi?id=179329	Bugzilla Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[50] Microsoft Security Bulletin, MS02-050 V2.2, September 5, 2002.
[51] Microsoft Security Bulletin, MS02-050 V4.0, November 20, 2002.
[52] Bugzilla Security Advisory, November 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla/ Netscape [53]	Multiple	Mozilla Browser 0.9.6-0.9.9, 1.0, 1.0.1, 1.1; Netscape 6.2- 6.2.3, 7.0	A buffer overflow vulnerability exists in the JAR URI handler due to insufficient checks, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Netscape/ Mozilla JAR Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Mozilla/ Netscape [54]	Windows 95/98/ME NT 4.0/2000, Unix	Mozilla Browser 1.0, 1.0 RC1&RC2, 1.0.1, 1.1, 1.1 Alpha & Beta, 1.2 Beta; Netscape Communicator 4.61, 4.72-4.79, 6.1, 6.2.3	An integer overflow vulnerability exists in the POP3 mail handler routines due to insufficient checks on server-supplied values, which could let a malicious user obtain control.	No workaround or patch available at time of publishing.	Netscape/ Mozilla POP3 Mail Handler Integer Overflow	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[55]	Unix	Solaris 2.5.1, 2.5.1 _x86, _ppc, 2.6, 2.6 _x86, 7.0, 7.0 _x86, 8.0, 8.0_x86, 9.0, 9.0_x86 Update 2; XFree86 X11R6 3.3, 3.3.2-3.3.5	A buffer overflow vulnerability exists in the XFS font server, fs.auto used by multiple vendors, which could let a remote malicious user execute arbitrary commands.	**XFree:** ftp://ftp.xfree86.org/pub/XFree86/4.2.0/Xinstall.sh Note: This is just the installation script. You must acquire the platform specific binary for this distribution from: ftp://ftp.xfree86.org/pub/XFree86/4.2.0/binaries/ or http://ftp.xfree86.org/pub/XFree86/4.2.0/binaries To determine which distribution you need to download, obtain the installation script (Xinstall.sh) and run the command: sh Xinstall.sh -check	Multiple Vendor fs.auto Remote Buffer Overrun	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[56, 57]	Unix	Astaro Security Linux 2.0 16, 23-27, 30, Linux 3.2 00, 10, 11; ISC BIND 4.9.2-4.9.10	A buffer overflow vulnerability exists in the DNS stub resolver library in the network name and address request functions, which could let a malicious user execute arbitrary code.	**ISC:** http://www.isc.org/products/BIND/patches/bind4910.diff	ISC BIND DNS Resolver Buffer Overflow CVE Name: CAN-2002-0029	**High**	Bug discussed in newsgroups and websites.

[53] Bugtraq, November 14, 2002.
[54] Bugtraq, November 26, 2002.
[55] ISS X-Force Security Brief, November 25, 2002.
[56] CERT® Advisory CA-2002-31, November 14, 2002.
[57] OpenPKG Security Advisory, OpenPKG-SA-2002.011, November 15, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NeoSoft Corp. [58]	Windows	NeoBook 4.0	A vulnerability exists in the 'NBActiveX.ocx' ActiveX control due to insufficient filtering of files, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	NeoBook 4 ActiveX Control	**High**	Bug discussed in newsgroups and websites.
NetBSD[59]	Unix	NetBSD 1.5-1.5.3, 1.6	A vulnerability exists because ftpd responds to the STAT command in a way that is not standards conformant, which could let a malicious user corrupt state tables in intermediate firewall devices and trick them into making unexpected TCP connections.	Upgrade available at: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-027.txt.asc	NetBSD ftpd Firewall State Table Corruption	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Netscape [60]	Multiple	Communicator 4.0, 4.5- 4.7, 4.51, 4.61, 4.72- 4.79	A vulnerability exists in the Java Virtual Machine (JVM) implementation of Netscape 4 browsers due to insecure calls to some methods, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Netscape Java Virtual Machine Insecure Cal	**High**	Bug discussed in newsgroups and websites.
Netscape [61]	Windows 95/98/ME/ NT 4.0/2000, Unix	Communicator 4.6, 4.61, 4.7, 4.72-4.78	A vulnerability exists because user preferences are stored in a predictable directory structure, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Netscape Predictable Directory Structure CVE Name: CAN-2002-1204	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Netscape [62]	Windows 95/98/ME/ NT 4.0/2000	Netscape Communicator 4., 4.5, 4.51, 4.6, 4.61, 4.7, 4.72-4.79	A vulnerability exists in the Java implementation due to an unchecked buffer in the method canConvert() of the class sun.awt.windows. WDefaultFontCharset, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Netscape Java canConvert() Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
NetScreen Technologies Inc.[63, 64]	Multiple	ScreenOS 3.1.0, 3.0.0, 1.7, 2.6, 2.8, 4.0	A vulnerability exists in the algorithms generating TCP initial sequence numbers that makes their selection predictable, which could let a malicious user inject malicious packets or launch a man-in-the-middle attack.	Upgrade available at: http://www.netscreen.com/support/updates.asp	ScreenOS Predictable Initial TCP Sequence Number	Medium	Bug discussed in newsgroups and websites.

[58] Bugtraq, November 16, 2002.
[59] NetBSD Security Advisory, 2002-027, November 19, 2002.
[60] Bugtraq, November 20, 2002.
[61] iDEFENSE Security Advisory, 11.19.02c, November 19, 2002.
[62] Bugtraq, November 26, 2002.
[63] NetScreen Security Alert 51929, November 25, 2002.
[64] NetScreen Security Alert 51897, November 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetScreen Technologies Inc.[65, 66]	Multiple	ScreenOS 3.1.1r2, 3.1.0r9, 3.1.0r1&r2, 3.1.0, 3.0.0r1-r4, 3.0.0, 2.8.0r1, 2.8, 3.0.1r1&r2, 3.0.3 r1.1, 4.0	A Denial of Service vulnerability exists due to the way H.323 control sessions are processed because H323 control sessions are not properly cleaned up.	Upgrade available at: http://www.netscreen.com/support/updates.asp	H.323 Control Session Denial Of Service	Low	Bug discussed in newsgroups and websites.
NetScreen Technologies Inc.[67]	Multiple	ScreenOS 3.1.1r2, 3.1.0r9, 3.1.0r2, 3.1.0r1, 3.1.0, 3.0.0r1-r4, 3.0.0, 2.8.0r1, 2.7.1 r1-r3, 2.7.1, 3.0.1 r1&r2, 4.0	A vulnerability exists in the 'Malicious-URL' blocking feature, which could let a malicious user bypass this feature.	Upgrade available at: http://www.netscreen.com/support/updates.asp	NetScreen Malicious URL Filter Bypassing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NullLogic [68]	Multiple	Null HTTPd 0.5, 0.5.1	A heap corruption vulnerability exists when a small content length value is submitted to the server, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Null HTTPD Remote Heap Corruption	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
nullmailer [69]	Unix	nullmailer 1.0 RC5	A Denial of Service vulnerability exists when mail is relayed to non-existent users.	**Debian:** http://security.debian.org/pool/updates/main/n/nullmailer/	Nullmailer Invalid User Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Open Webmail [70]	Unix	Open Webmail 1.70, 1.71	A vulnerability exists during the authentication process when an invalid username is entered, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Open WebMail Invalid Unsername	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
OpenBSD [71]	Unix	OpenBSD 2.9-3.2	A vulnerability exists in the remote reporting functionality of syslogd when a host reconfigures its IP address and doesn't reboot, which could let a remote syslogd server receive false information.	No workaround or patch available at time of publishing.	OpenBSD False syslogd Source IP Reporting	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[65] NetScreen Security Alert 51929, November 25, 2002.
[66] NetScreen Security Alert 52020, November 25, 2002.
[67] NetScreen Security Alert 51929, November 25, 2002.
[68] SecurityFocus, November 26, 2002.
[69] Debian Security Advisory, DSA 198-1, November 18, 2002.
[70] Securiteam, November 24, 2002.
[71] Bugtraq, November 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software[72]	Windows, MacOS, Unix	Opera Web Browser 7.0 win32 Beta 1	Two unspecified vulnerabilities exist which could let a remote malicious user obtain sensitive information and execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Unspecified Opera 7 Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Opera Software[73]	Unix	Opera Web Browser 6.0.3 Linux	A Denial of Service vulnerability exists when an HTTPS proxy is used after the certificate has been accepted.	No workaround or patch available at time of publishing.	Opera HTTPS Proxy Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Perception [74]	Windows NT	LiteServe 2.0, 2.0.1, 2.0.2	A vulnerability exists due to the way filenames are handled on Win32 platforms, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	LiteServe CGI Source Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Perception [75]	Windows NT	LiteServe 2.0, 2.0.1, 2.0.2	A buffer overflow vulnerability exists when a malformed GET request is submitted, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	LiteServe Malformed GET Request Buffer Overflow	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP Evolution [76]	Unix	News Evolution 1.0, 2.0	A vulnerability exists in the 'aff_news.php' and 'export_news.php' files, which could let a malicious user obtain sensitive information. and execute arbitrary commands.	No workaround or patch available at time of publishing.	News Evolution Include Undefined Variable Command Execution	Medium **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
phpBB Group[77]	Unix	phpBB 2.0.3	A Cross-Site Scripting vulnerability exists in some of the scripts, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PHPBB2 ViewTopic. PHP Cross Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
phpBB Group[78]	Unix	phpBB 2.0.3	A vulnerability exists due to improper sanitization of user input in forum postings, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	phpBB Forum Postings	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[72] SecurityTracker Alert ID, 1005634, November 14, 2002.
[73] SecurityFocus, November 21, 2002.
[74] Securiteam, November 18, 2002.
[75] SecurityFocus, November 18, 2002.
[76] SecurityFocus, November 29, 2002.
[77] Bugtraq, November 18, 2002.
[78] Sec-Tec Advisory, November 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Phystech[79]	Unix	dhcpcd 1.3.22 -pl1	A vulnerability exists in '/sbin/dhcpd-<interface>.exe'. when assigning an IP address to a network interface, which could let a remote malicious DHCP server execute arbitrary shell commands. This is an optional configuration that must be setup manually by copying the script into /sbin/.	**Phystech:** http://www.phystech.com/download/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	DHCPCD Character Expansion Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
Portail PHP[80]	Unix	PortailPHP 0.99	A vulnerability exists in the mod_search module due to insufficient sanitization of variables used to construct SQL queries in the 'index.php' script, which could let a malicious user corrupt database information.	No workaround or patch available at time of publishing.	PortailPHP SQL Injection	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Pserv[81]	Multiple	Pserv 2.0 beta 1-beta 3	A buffer overflow vulnerability exists when a malicious HTTP POST request is submitted, which could let a malicious user cause a Denial of Service and possible execute arbitrary code.	No workaround or patch available at time of publishing.	Pserv HTTP POST Request Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
pWins[82]	Windows, Unix	pWins 0.2.5	A Directory Traversal vulnerability exists due to a failure to sanitize web requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	pWins Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
QNX Software Systems Ltd.[83]	Unix	Photon MicroGUI	A vulnerability exists in the clipboard feature because data is not stored securely when copied to the clipboard, which could let al malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	QNX Photon MicroGUI Clipboard Insecure Data Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
QNX Software Systems Ltd.[84]	Unix	RTOS 6.2.0 Update Patch A, 6.2 .0	A configuration vulnerability exists because several executable files are configured with unsafe permissions, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	QNX Multiple Program Insecure Default Permissions	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[79] Conectiva Linux Security Announcement, CLA-2002:549, November 18, 2002.
[80] SecurityFocus, November 28, 2002.
[81] INetCop Security Advisory, 2002-0x82-005, November 24, 2002.
[82] SecurityTracker Alert ID, 1005726, November 28, 2002.
[83] Securiteam, November 24, 2002.
[84] Securiteam, November 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Rational Software[85]	Unix	ClearCase 2002.05, 4.1	A Denial of Service vulnerability exists when a remote malicious user submits two consecutive portscans.	Patches available at: http://www.rational.com/techsupport/clearcase/tech/patchlink/new/clearcase/2002.05.00/	ClearCase Portscan Denial of Service	Low	Bug discussed in newsgroups and websites Proof of Concept exploits have been published.
Real Networks[86]	Windows 95/98/NT 4.0/2000, XP	RealOne Player 2.0, G2, 6.0 Win32, 7.0 Win32, 8.0 Win32	Multiple buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists when a malicious Synchronized Multimedia Integration Language (SMIL) file is constructed, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in the "Now Playing" menu when an overly long rtsp:// filename parameter is supplied, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists when viewing malicious RealFlash presentations, which could let a malicious user corrupt memory.	Patch available at: http://service.real.com/help/faq/security/07092002/skinpatchr11s.rmp *Note: reports indicate that the patch supplied by Real Networks for this issue does not rectify the problem.*	RealOne Player Buffer Overflow Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Rich Media Technologies[87]	Windows 98/ME/2000	JustAdd Commerce Standard 5.0	A vulnerability exists due to insufficient validation of hidden form field information, which could let a malicious user manipulate sensitive information.	No workaround or patch available at time of publishing.	JustAdd Commerce Insufficient Validation Hidden Form Field	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[85] Guardeonic Solutions AG Security Advisory, 03-2002, November 22, 2002.
[86] NGSSoftware Insight Security Research Advisory, NISR22112002, November 22, 2002.
[87] WhiteHat Security Advisory 1004, November 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Samba[88, 89, 90, 91, 92, 93, 94]	Unix	Samba 2.2.2-2.2.6	A buffer overflow vulnerability exists in a function used to decrypt hashed passwords due to insufficient bounds checking of user-supplied input, which could let a malicious user execute arbitrary code with super user privileges.	**Samba:** http://download.samba.org/samba/ftp/ **RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/1.5/RPMS/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **SuSE:** ftp://ftp.suse.com/pub/suse/ **Debian:** http://security.debian.org/pool/updates/main/s/samba/	Samba Server Encrypted Password Buffer Overrun	**High**	Bug discussed in newsgroups and websites.
SSH Communications Security[95]	Unix	SSH2 2.0.13, 2.1-2.5, 3.0, 3.0.1, 3.1- 3.1.4, 3.2, 3.2.1	A vulnerability exists because the setsid() function fails to remove the child from the parent process group, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://ftp.ssh.com/priv/secureshell/h7cq89th/	SSH Server Privilege Escalation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
SSH Communications Security[96]	Windows	SSH2 3.1, 3.1.1-3.1.4, 3.2	A buffer overflow vulnerability exists in the Secure Shell Windows client due to an error in the URL handling, which could let a malicious user execute arbitrary code.	Upgrade available at: http://ftp.ssh.com/priv/secureshell/h7cq89th	Secure Shell Windows Client URL Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[97]	Windows NT 4.0/2000, Unix	iPlanet Web Server 4.1, 4.1 SP1-SP11	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists when administrative logs are viewed on the iPlanet Admin server, and a vulnerability exists in the Admin Server's PERL pages used for administrative tasks due to insecure calls to the open() function. Using the combination of the two vulnerabilities could let a remote malicious user execute arbitrary HTML and script code as root.	No workaround or patch available at time of publishing.	iPlanet Admin Cross-Site Scripting & Unsafe Perl Script open() Calls	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[88] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:266-05, November 22, 2002.
[89] Conectiva Linux Security Announcement, CLA-2002:550, November 22, 2002.
[90] SuSE Security Announcement, SuSE-SA:2002:045, November 20, 2002.
[91] Gentoo Linux Security Announcement , 200211-007, November 21, 2002.
[92] Debian Security Advisory, DSA-200-1, November 22, 2002.
[93] Mandrake Linux Security Update Advisory, MDKSA-2002:081, November 26, 2002.
[94] Trustix Secure Linux Security Advisory, 2002-0080, November 25, 2002.
[95] SSH Communications Advisory, November 25, 2002.
[96] SSH Communications Security Advisory, November 25, 2002.
[97] Next Generation Security Technologies Security Advisory, November 19, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[98] ***Upgrade now available and exploit script published***[99]	**Unix**	**Cobalt Control Station 4100CS, Cobalt Qube3 4000WG, Qube3 w/ Caching & RAID 4100WG, Qube3 w/Caching 4010WG, RaQ XTR 3500R, RaQ4 3001R, RaQ4 RAID 3100R**	**A vulnerability exists in /usr/lib/authenticate, which could let a malicious user obtain root privileges.**	***Upgrade available at:*** http://ftp.cobalt.sun.com/pub/packages/	**RaQ authenticate Root Privilege Escalation**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Sun Micro-systems, Inc.[100]	Unix	Solaris 2.5.1, 2.6, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	A Directory Traversal vulnerability exists in priocntl() when accessing a module due to a failure to sanitize module names, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Solaris priocntl() System Call Local Root	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun/ Netscape[101]	Windows, Unix	Netscape Communi-cator 4.0-4.8; Sun Java 2 Runtime Environ-ment 1.1-1.4	A vulnerability exists due to a flaw in the Bytecode Verifier, which could let a remote malicious user obtain unauthorized access and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Sun/Netscape Java Virtual Machine Bytecode Verifier	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[98] Sun(sm) Alert Notification, 46988, September 10, 2002.
[99] SecurityFocus, November 25, 2002.
[100] Bugtraq, November 27, 2002.
[101] SecurityTracker Alert IDs, 1005701 & 1005702, November 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SuSE[102] ***Debian issues advisory***[103] ***Exploit script has been published***[104]	**Unix**	**Linux 7.0-7.3, 8.0, 8.1**	**Two vulnerabilities exist: a vulnerability exists in the 'runlpr' utility when malicious strings are passed via the commandline which could allow a malicious user to execute arbitrary commands; and a vulnerability exists in the html2ps filter that is included in the lprng print system, which could let a remote malicious user execute arbitrary commands.**	**Patches available at:** **ftp://ftp.suse.com/pub/suse/** ***Debian:*** **http://security.debian.org/pool/updates/main/h/html2ps/**	**LPRNG Runlpr & html2ps Command Execution**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Sybase[105]	Windows NT 4.0, Unix	Adaptive Server Enterprise 12.0 Win, 12.0 Sun, 12.0 HP, 12.5 Win, 12.5 Sun, 12.5 HP, 12.5 SGI, 12.5 Digital UNIX	A buffer overflow vulnerability exists in the DBCC CHECKVERIFY function due to insufficient checks on the length of the string that is supplied as input when the function is called, which could let a local/remote malicious user obtain root privileges.	Patch available at: http://downloads.sybase.com/swd/swx	Adaptive Server DBCC CHECK VERIFY Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sybase[106]	Windows NT 4.0, Unix	Adaptive Server Enterprise 12.0 Win, 12.0 Sun, 12.0 HP, 12.5 Win, 12.5 Sun, 12.5 HP, 12.5 SGI, 12.5 Digital UNIX	A buffer overflow vulnerability exists in the built-in function DROP DATABASE due to insufficient checks on the length of the string that is supplied as input when the function is called, which could let a local/remote malicious user obtain root privileges.	Patch available at: http://downloads.sybase.com/swd/swx	Adaptive Server DROP DATABASE Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sybase[107]	Windows NT 4.0	Adaptive Server Enterprise 12.0 Win, 12.5 Win	A buffer overflow vulnerability exists in the xp_freedll extended stored procedure due to insufficient checks on the length of the string that is supplied as input when the function is called, which could let a local/remote malicious user obtain root privileges.	Patch available at: http://downloads.sybase.com/swd/swx	Adaptive Server xp_freedll Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[102] SuSE Security Announcement, SuSE-SA:2002:040, October 31, 2002.
[103] Debian Security Advisory, DSA 192-1, November 8, 2002.
[104] SecurityFocus, November 25, 2002.
[105] SHATTER Team Security Alert, November 26, 2002.
[106] SHATTER Team Security Alert, November 26, 2002.
[107] SHATTER Team Security Alert, November 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symantec[108]	Multiple	Java! JustInTime Compiler 210.65	A vulnerability exists in the Java! JustInTime compiled used by Netscape Communicator, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Symantec Java! JustInTime Compiler Command Execution	High	Bug discussed in newsgroups and websites.
TFTPD32[109]	Windows 95/98/NT 4.0/2000, XP	TFTPD32 2.50, 2.50.2	A Directory Traversal vulnerability exists which could let a remote malicious user download/upload arbitrary system files and possibly replay key system files with Trojaned copies.	Upgrade available at: http://perso.wanadoo.fr/philippe.jounin/download/tftpd32j.zip	TFTPD32 Arbitrary File Download/ Upload	High	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
TFTPD32[110]	Windows 95/98/NT 4.0/2000, XP	TFTPD32 2.50, 2.50.2	A buffer overflow vulnerability exists due to insufficient checks on user-supplied input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://perso.wanadoo.fr/philippe.jounin/download/tftpd32j.zip	TFTPD32 Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
TuxBR[111]	Unix	LIBCGI 1.0.2, 1.0.3	A buffer overflow vulnerability exists in the 'parse_field()' function in the 'cgi_lib.c' source file due to insufficient bounds checking of user-supplied input, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	LIGCGI Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Web Server Creator[112]	Multiple	Web Server Creator Web Portal 0.1	A vulnerability exists in the 'customize.php' and 'index.php' scripts because it is possible to influence the include path, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Web Server Creator Web Portal Remote File Include	High	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Working Resources Inc.[113]	Multiple	BadBlue 1.7.1	A Cross-Site Scripting vulnerability exists because the ext.dll ISAPI does not sufficiently sanitize user-supplied input when processing search queries, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Working Resources BadBlue Search Page Cross Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Working Resources Inc.[114]	Windows NT	BadBlue 1.7.1	An information disclosure vulnerability exists in the 'soinfo.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BadBlue Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[108] Bugtraq, November 20, 2002.
[109] Bugtraq, November 18, 2002.
[110] Bugtraq, November 18, 2002.
[111] Securiteam, November 28, 2002.
[112] SecurityFocus, November 25, 2002.
[113] Bugtraq, November 24, 2002.
[114] Securiteam, November 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WSMP3 [115]	Multiple	WSMP3 .1, .2	Several buffer overflow vulnerabilities exist due to improper bounds checking when data is copied to local buffers, which could let a remote malicious user execute arbitrary code; and a heap corruption vulnerability exists due to insufficient bounds checking of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WSMP3 Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Exploit script has been published for the heap corruption vulnerability.
YaBB[116]	Unix	YaBB 1 Gold - SP 1	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of URI parameters in some scripts, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	YaBB.pl Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Zeus Technologies[117] ***Upgrade now available*** *[118]*	**Multiple**	**Zeus Web Server 4.1r2**	**A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary HTML and script code.**	***Upgrade available at: http://www.zeus.com/downloads/***	**Zeus Web Server Cross-Site Scripting**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[115] INetCop Security Advisory, 2002-0x82-006, November 25, 2002.
[116] SecurityFocus, November 28, 2002.
[117] Bugtraq, November 8, 2002.
[118] SecurityFocus, November 26, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 16 and November 30, 2002, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 41 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 30, 2002	Ex_pfinger.c	Script that exploits the Pfinger Root vulnerability.
November 30, 2002	Traceroute-exploit.c	Script that exploits the Traceroute-Nanog Buffer Overflow Vulnerabilities.
November 28, 2002	**0x82-Remote.tuxbrlibcgi.s**	**Exploit for the LIGCGI Buffer Overflow vulnerability.**
November 27, 2002	**0x82-libcgifpxpl.c**	**Script that exploits the Lib CGI Include Buffer Overflow vulnerability.**
November 27, 2002	**Final.c**	**Script that exploits the Solaris priocntl() System Call Local Root vulnerability.**
November 27, 2002	**Flkm.c**	**Script that exploits the Solaris priocntl() System Call Local Root vulnerability.**
November 25, 2002	Html2shell	Exploit for the LPRNG Runlpr & html2ps Command Execution vulnerability.
November 25, 2002	**Vbulletinxss-exp.txt**	**Technique for exploiting the VBulletin members2.php Cross-Site Scripting vulnerability.**
November 25, 2002	**Wsmp3xpl.c**	**Script that exploits the WSMP3 Multiple Vulnerabilities.**
November 24, 2002	Anwrap.pl	A dictionary attack tool that can be used against LEAP enabled CiscoWireless Networks.
November 24, 2002	Hudo.c	Linux exploit for versions of sudo 1.6.3p7 and below. Very detail exploitation instructions included.
November 24, 2002	**SF-talkischeap.pl**	**Script that exploits the Internet Talker Remote Denial of Service vulnerability.**
November 23, 2002	Hydra-2.2.tar.gz	A parallel login malicious user tool that enables you to attack several services at once (Samba, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, VNC, ICQ, Socks5, PCNFS, Cisco and more).
November 23, 2002	Networkactivscannerv4.0.exe	Advanced network scanner with many useful features that can perform DNS dig, whois, and more.
November 23, 2002	**Zerooexploit.txt**	**Exploit for the Zeroo HTTP Server Remote Buffer Overflow vulnerability.**
November 21, 2002	**Mailenable-dos.c**	**Script that exploits the MailEnable E-mail Server Buffer Overflow vulnerability.**
November 21, 2002	Raqfuck.sh	Script that exploits the RaQ authenticate Root Privilege Escalation vulnerability.
November 21, 2002	**Vbulletin-xss.php**	**Exploit for the VBulletin Cross-Site Scripting vulnerability.**
November 19, 2002	**Iplanet-ngxss.sh**	**Exploit for the iPlanet Admin Cross-Site Scripting & Unsafe Perl Script open() Calls vulnerability.**
November 19, 2002	Paketto-1.0.tar.gz	Scanrand implements extremely fast and efficient port, host, and network trace scanning that uses cryptographic signatures.
November 19, 2002	Sql2.cpp	Script that exploits the MSSQL Server 2000 SP0 buffer overflow vulnerability.
November 19, 2002	Tftpd32.pl	Perl script that exploits the TFTPD32 Buffer Overflow vulnerability.
November 18, 2002	**Liteservexpl.pl**	**Perl script that exploits the LiteServe CGI Source Disclosure vulnerability.**

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 18, 2002	**Sfexpl.zip**	**Exploit for the Flash SWRemote Heap Corruption vulnerability.**
November 18, 2002	Spikeproxy-1.4.6.tar.gz	A web application analysis tool that uses the SPIKE API to help reverse engineer new and unknown network protocols.
November 18, 2002	Tftpd32-exploit.pl	Perl script that exploits the TFTPD32 Buffer Overflow vulnerability.
November 17, 2002	Iisunicodeexplained.doc	A paper that goes into detail on Unicode exploitation with how it works and how to actually perform attacks against IIS servers that are vulnerable to this bug.
November 16, 2002	**0x82-Zer00.sh**	**Script that exploits Zeroo HTTP Server Remote Buffer Overflow vulnerability.**
November 16, 2002	Amnesia.pl	An encryption/decryption tool for files and directories that uses a 702 bit key built off of a user provided password.
November 16, 2002	Core_vulnerabilities.pdf	A paper that underlines some of the most common mistakes made by programmers, presented as ten examples and shows the exact location of vulnerabilities in codes, providing detailed explanations and exploits for each one found.
November 16, 2002	Ex_cifslogin.c	Script that exploits the cifslogin vulnerability.
November 16, 2002	Exploitipppd.c	Script that exploits the isdn4linux ipppd vulnerability.
November 16, 2002	Mapper-2.19.tar.gz	A network connectivity tester that employs a number of techniques to try and guess if a host is alive or not.
November 16, 2002	Psibrute.com.txt	A DCL script that abuses the old psi_mail trick on VAX/VMS systems to remotely find valid users.
November 16, 2002	Savantslap.zip	Denial of Service exploit for Savant HTTP Server vulnerability.
November 16, 2002	Smtpscan-0.3.tar.gz	A tool that guesses which MTA is used by sending several "special" SMTP requests and by comparing error codes returned with those in the fingerprint database.
November 16, 2002	Sorsync.c	Remote exploit for the rsync vulnerability.
November 16, 2002	Tinywebug.txt	Technique for exploiting the Tiny HTTPd vulnerability.
November 16, 2002	Winfingerprint-0.5.4.zip	Advanced remote windows OS detection that determines OS using SMB Queries, PDC (Primary Domain Controller), BDC (Backup Domain Controller), NT member server, NT workstation, qlserver, novell netware server, windows for workgroups, windows 9X, Enumerate Servers, Enumerate Shares including Administrative ($), Enumerate Global Groups, E numerate Users, Displays Active Services, Ability to Scan Network Neighborhood, Ability to establish NULL IPC$ session with host, Ability to Query Registry (currently determines Service Pack Level & Applied Hotfixes.
November 16, 2002	Wininterrogate-0.1.5.zip	Winterrogate recurses directory structure obtaining the following information according to filemask: File Name, Complete Path, Directory, File Size, Creation Time, Last Access Time, Last Write Time, and MD5 Checksum.
November 16, 2002	**Zeroobug.txt**	**Exploit for the Zeroo HTTP Server Remote Buffer Overflow vulnerability.**

Trends

- **The Internet security community has identified several new vulnerabilities in the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) software, which is used by many ISPs to provide DNS services. The National Infrastructure Protection Center (NIPC) is issuing this advisory to heighten awareness to three newly identified vulnerabilities in BIND versions 4 and 8. For more information see NIPC Advisory 02-009, located at: http://www.nipc.gov/warnings/advisories/2002/02-009.htm and "Bugs, Holes & Patches" table.**
- **The CERT/CC has received reports that an intruder modified several of the released source code distributions of the libpcap and tcpdump packages and contain a Trojan horse. For more information see CERT® Advisory CA-2002-30, located at: http://www.cert.org/advisories/CA-2002-30.html and "Bugs, Holes & Patches" table.**
- **Multiple Kerberos distributions contain a remotely exploitable buffer overflow in the Kerberos administration daemon, which could let a remote malicious user obtain root privileges. The CERT/CC has received reports that indicate that this vulnerability is being exploited. For more information, see "Bugs, Holes & Patches" Table and CERT Advisory, CERT® Advisory CA-2002-29, located at: http://www.cert.org/advisories/CA-2002-29.html.**
- **There have been a significant number of calls from customers concerned about a widespread e-mail that invites users to pick up an "E-Card" from a website called FriendGreetings.com. For more information, see http://www.sophos.com/virusinfo/articles/greetings.html.**
- **Firewalls and other systems that inspect FTP application layer traffic may not adequately maintain the state of FTP commands and responses. As a result, an attacker could establish arbitrary TCP connections to FTP servers or clients located behind a vulnerable firewall. For more information see Vulnerability Note VU#328867, located at: http://www.kb.cert.org/vuls/id/328867.**
- **The CERT/CC has received confirmation that some copies of the source code for the Sendmail package have been modified by an intruder to contain a Trojan horse. For more information, see "Bugs, Holes, & Patches Table" and CERT® Advisory CA-2002-28 located at: http://www.cert.org/advisories/CA-2002-28.html.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of an e-mail-borne worm known as W32.Bugbear or I-Worm.Tanatos. For more information, see NIPC Advisory 02-008, located at: http://www.nipc.gov/warnings/advisories/2002/02-008.htm and Virus Section.**
- **The National Infrastructure Protection Center (NIPC) has been coordinating with the anti-virus and security community on the life cycle of "Slapper," the OpenSSL/Apache worm and all its variants. For more information, see NIPC ASSESSMENT 02-003, located at: http://www.nipc.gov/warnings/assessments/2002/02-003.htm.**
- **The SANS Institute and the National Infrastructure Protection Center (NIPC) have updated the list containing the Twenty Most Critical Internet Security Vulnerabilities. This list is broken into two categories: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. For more detailed information, see: http://www.sans.org/top20.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Stable	January 2002
2	W32/Bugbear-A	Worm	Stable	September 2002
3	Elkern	File Infector	Slight Increase	October 2001
4	**W32/Yaha**	Worm	Slight Decrease	February 2002
5	W32/Nimda-A-O	File, Worm	Slight Decrease	September 2001
6	I-Worm.Sircam	Worm	Slight Increase	July 2001
7	I-Worm.Magistr	File, Worm	Slight Decrease	March 2001
8	JS/NoClose	Trojan	Slight Increase	May 2002
9	W32/Hybris	File, Worm	Slight Decrease	November 2000
10	Funlove	File	Slight Decrease	November 1999

Note: Virus reporting may be weeks behind the first discovery of infection. A total 201 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 374 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

BAT_BONG.A (Batch File Worm): This batch file malware uses its Visual Basic Script component to send copies of itself to all e-mail addresses found in the infected user's Microsoft Outlook address book. It also has IRC file components that send it to all mIRC and Pirch users that join infected users' current Internet Relay Chat channels. The details of the e-mail message that it sends out are as follows:

- Subject: An attachment.
- Message Body: II would like to show you the work that I want to give to you. This is the installer. Bye!!
- Attachment: gong.bat

The worm overwrites the system file, AUTOEXEC.BAT, so that it is executed on startup.

BAT_DGAM.A (Batch File Worm): This destructive batch file worm propagates by sending copies of itself via e-mail to all addresses listed in the default Global Address Book of the infected system. It deletes the critical system file REGEDIT.EXE and overwrites AUTOEXEC.BAT with malicious codes. It also drops a Visual Basic Script (VBS) file, VBS_DGAM.A, to facilitate its mass-mailing routine. This VBS component sends out a copy of the worm in an e-mail with the following details:

- Subject: Greeting card for you!
- Message Body: Hi! How are you? I am sending you this greeting card because I miss you so much. Enjoy!
- Attachment: E-CARD.SWF.BAT

This worm also disables the Run command in the Start Menu button and disables the use of any registry tools such as REGEDIT.EXE.

VBS.Cepic@mm (Visual Basic Script Worm): This is a simple mass-mailing worm that is written in the Visual Basic Scripting (VBS) language. When VBS.Cepic@mm is executed, it attempts to create a copy of itself as %system%\Lebensretter2002.vbs. Next, the worm attempts to delete the file, C:\Windows\Netstat.exe, and adds the value, “Lebensretter2002 %system%\Lebensretter2002.vbs,” to these registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

so that the worm runs when you start Windows. Finally, the worm attempts to e-mail all contacts in the Microsoft Outlook Address Book. The worm will only e-mail up to the first 100. The message that the worm sends is as follows:

- Subject: Nice Pics 4 U
- Message Body: Only open the file and enjoy :)
- Attachment: Nicepics.jpg.vbs

VBS/Cybarm.a (Visual Basic Script Virus): On execution, the virus will copy itself as Kernel32.vbs in windows SYSTEM directory. The virus will also make a copy of itself as "ISO9" + [second] + [minute].exe.vbs. An example of a filename it may create depending on the second and minute would be: IS091942.exe.vbs. This file is created to the hard coded directory C:\Windows\Desktop. The virus also creates MyAdult + [minute].jpg.vbs in all network directories. If X97M/Yawn.n@MM dropped the script, the file C:\army.xls will also be copied to all network drives.

VBS_FOPHACK.A (Alias: VBS/FOPHACK-A) (Visual Basic Script Worm): This encrypted Visual Basic Script malware spreads using Microsoft Outlook. It sends e-mail with itself as attachment to all addresses found in the infected user's address book. The e-mail message that it sends out has the following details:

- Subject: XXX Picture For You!
- Message Body: To view the XXX picture, you need to download an attachment. Enjoy!
- Attachment: XXX-GIRLS-FOR-YOU.jpg.vbs

After mass mailing, it sends a notification e-mail to melhacker83@hotmail.com with the following details:

- Subject: MISSION ACCOMPLISHED MELHACKER
- Message Body: Dear Sir, The virus are already infected.

It searches for a directory that has a name with the string “WIN” and then drops a copy of itself in this directory as SYSMEl32.EXE.VBS.

VBS.Hypoth@mm (Visual Basic Script Worm): This is a mass-mailing worm that uses Microsoft Outlook to e-mail itself. It infects .vbs and .vbe files and renames audio and video files.

VBS.Zsyang@mm (Aliases: I-Worm.Zsyang, VBS/Zsyang.A@mm) (Visual Basic Script Worm): VBS.Zsyang@mm is a Visual Basic Script that mails itself to all contacts in your address list. The worm also carries a payload that destroys all data on the computer. It arrives in an e-mail message that has the following characteristics:

- Subject: WebMaster Report
- Message: Your E-mail address is wrong. Please check it.
- Attachment: Cry.vbs

When VBS.Zsyang@mm runs, it tries to modify the (Default) value of the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

to the Value data, C:\Windows\System\Cry.vbs, and then creates a copy of itself in C:\Windows\System\. If the registry value under the registry key:

- HKEY_CURRENT_USER\Software\h&d

does not contain the Value data 1, then VBS.Zsyang@mm mails itself to all contacts in your Address Book and sets the value to 1 . VBS.Zsyang@mm also creates a shell window that tries to format drive E. Finally, VBS.Zsyang@mm replaces (or creates) the content of C:\Autoexec.bat with a line that calls the Format command and directs it to format drive C the next time that you restart the computer.

W32.Fusic@mm (Win32 Worm): This is a mass-mailing worm with backdoor capabilities that replicates by e-mail. It uses MAPI to send itself to the contacts in the Windows Address Book. When W32.Fusic@mm runs, it copies itself as %system%\Kernel\Kernel32.exe and creates the following files:

- %system%\FuncDLL.dll
- %system%\IEHelper.dll

Both .dll files are used by the Trojan component to intercept keystrokes. FuncDLL.dll can intercept keystrokes by hooking keyboard messages. IEHelper.dll can handling Internet Explorer events that are triggered by the browser whenever you enter data into input fields. Both file log intercepted data and the URL into %system%\Passlogx.log. The presence of this file may indicate the infection, and you can, if needed, look at the file to determine what information was intercepted. Both .dll files are detected as PWS.Hooker.Trojan. The worm creates the value, "kernel   %system%\kernel\kernel32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the worm starts when you start or restart Windows. Also, it creates the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\kernel
- HKEY_LOCAL_MACHINE\SOFTWARE\kernel\A09b37xz

The keys contain values that store internal configuration data. If the operating system is Windows 95/98/ME, the worm registers itself as a service process to continue to run after you log off. In this case, W32.Fusic@mm will close only when the system is shut down. The worm installs hook procedures into a hook chain to monitor the system for any keyboard and mouse messages. The keyboard and mouse hook procedures process the messages and pass the hook information to the next hook procedure in the current hook chain. This permits W32.Fusic@mm to intercept any keystrokes. Once installed, W32.Fusic@mm waits for commands from the remote client. The commands allow the malicious user to perform various actions. The worm inventories contacts in the Windows Address Book and sends itself using MAPI. If it cannot locate the address book file, it tries to obtain the location of Wab32.dll. Then it loads that .dll and calls WABOpen() to open the Address Book. Next, the worm checks the Locale ID.

W32/GOP.j@MM (Win32 Worm): This mass-mailer arrives as an attachment with a double-extension. The e-mail message contains a variable Chinese subject and message body, but may use an English message body, carried within the virus body, that is reminiscent of the Friend Greeting application. The message header is also malformed to exploit the Incorrect MIME Header (MS01-020) vulnerability Therefore, it will automatically run on an unpatched system when the message is viewed in Microsoft Outlook or Outlook Express. When run, the worm extracts an embedded file taken from the sender's system (a .bmp, .doc, .gif, .jpeg, .jpg, .rtf, or .txt file) to the WINDOWS TEMP directory and opens it. The name of this embedded file makes up the first part of the attachment name (i.e. SURVEY.DOC.EXE). The worm then copies itself to the WINDOWS SYSTEM (%SysDir%) directory as windowsagent.exe, and creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WindowsAgent=C:\WINDOWS|\SYSTEM\WINDOWSAGENT.EXE

An ICQ password-stealing component is also created and is saved to the WINDOWS and\or WINDOWS SYSTEM directory as drocerrbk.sys.

W32/Holar.b@MM (Win32 Worm): This mass-mailing worm spreads via e-mail, visiting an infected website, and network shares. It arrives as an attachment with a .SCR extension. The filename is chosen by selecting the filename (without the extension) of a file in the My Documents directory on the infected system. The subject of the message is the same as the filename but without the extension. The worm exploits the Incorrect MIME Header Can Cause IE to Execute E-mail Attachment vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), to automatically execute the virus on vulnerable systems. The message body contains the text Flash File and the attachment icon is that typically associated with a Shockwave Flash file. When the attachment is run, the worm copies itself to the WINDOWS SYSTEM directory and creates a registry run key to load itself at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\ZaCker

The .A variant of this threat dropped a webserver in the System directory as "CmdServ.exe" and an additional registry run key is created for it:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\MyLife=C:\WINDOWS\SYSTEM\CmdServ.exe

This variant creates the registry entry, but not the server file itself. This variant appends .HTM, and .HTML files to contain an IFrame that links to the file "C:\WINDOWS\SYSTEM\WarIII.eml," a copy of the worm. Additional registry keys are created as markers for the worm, for it to know if certain actions have taken place:

- HKEY_LOCAL_MACHINE\Software\Microsoft\HolyWar
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HolyWar

W32.Stopin@mm (Win32 Worm): This is a mass-mailing worm that uses the default e-mail program (as indicated in the registry) to send itself to all e-mail addresses in the e-mail program's inbox. The e-mail message has the following characteristics:

- Subject: Re: <the subject line of the incoming e-mail>
- Attachment: The attachment contains a file that has two extensions (ending in .exe, .pif, .scr or .com).

The threat is written in the Microsoft C++ programming language.

W32.Valla.2048 (Win32 Virus): This virus infects Win32 files by appending the virus code to the host. When it is executed, this virus infects Win32 executable files in the %windir% and %system% folders. It infects files by adding a new section named "XOR" at the end of the last section of the host, and it appends the virus code to the host.

W32/Winevar-A (Aliases: I-Worm.Winevar, WORM_WINEVAR.A, W32/Korvar, Worm/Bride.C, W32.HLLW.Winevar, W32/Winevar@mm) (Win32 Worm): This worm has been reported in the wild. It is a dropper for the W32/Flcss virus and a worm that spreads by e-mailing itself via SMTP to addresses on the local computer. The worm copies itself to the Windows system folder as WINXXXX.PIF (where XXXX represents a random four-digit number) and adds to the following registry entries to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

The worm also drops a copy of itself on the Windows Desktop as EXPLORER.PIF. W32/Winevar-A drops W32/Flcss within the Windows system folder as WINXXXX.TMP (where XXXX represents a random four-digit number). The file contains the following text within its DOS header: "~ AAVER 2002 in Seoul ~." E-mails have the following characteristics:

- From: <registered owner> (defaults to "AntiVirus")
- Subject: <registered organisation> (defaults to "Trand Microsoft Inc.") or Subject: Re: AVAR (Association of Anti-Virus Asia Researchers)
- Attached files:
  WINXXXX.TXT (12.6 KB)MUSIC_1.HTM
  WINXXXX.GIF (120 BYTES) MUSIC_2.CEO
  WINXXXX.PIF

W32/Winevar-A creates several entries within the registry at HKCR\Software\Microsoft\DataFactory, which is a repository of the addresses to which an infected e-mail has been sent. The HTM file contains a link entitled "Association of Ti-Virus Asia Researchers" which points to www.aavar.org. When run, the HTM file adds an entry to the registry so that CEO files are interpreted as EXE files by the operating system. W32/Winevar-A attempts to terminate processes containing the following names: view, debu, scan, mon, vir, iom, ice, anti, fir, prot, secu, dbg, avk, pcc, spy, microsoft, ms, _np, r n, cicer, irmon, smtpsvc, moniker, office, program, explorewclass, antivirus, cillin, nlab, vacc. This appears to be an attempt to disable various anti-virus products that may be running on the infected user's computer. On system restart W32/Winevar-A displays the message "Make a fool of oneself: What a foolish thing you've done!." If the "OK" button is pressed the worm deletes all deleteable files in all folders. W32/Winevar-A also attempts to launch a Denial of Service attack on the website belonging to anti-virus vendor Symantec by sending HTTP requests to www.symantec.com every 1 millisecond in an infinite loop.

WORM_BRAID.B (Aliases: W32/Braid.b@MM, BRID.B, WORM_BRAID.B.EML) (Internet Worm): This worm drops copies of itself in the Windows Desktop directory. It sends copies of itself via Simple Mail Transfer Protocol (SMTP) to all e-mail addresses listed in .HTM and .DBX files on the infected system. It sends e-mail with the following details:

- From: <Registered Windows Owner>
- Subject: <Registered Owner Organization>
- Attachment: README.EXE (90,111 Bytes)

The FROM field may display the recipient's e-mail address. Also, checking the e-mail address under the properties section for the displayed registered owner name should reveal the recipient's e-mail address. Due to programming errors, this worm is unable to function properly and propagate on Windows NT and 2000 systems.

WORM_FREGIT.B (Aliases: Win32/Fregit.B@mm, W32/Fregit.b@MM) (Internet Worm): This is a variant of WORM_FREGIT.A. This non-destructive, memory-resident, non-encrypted, worm uses Microsoft Outlook to send itself as attachment to an e-mail message that it sends to all addresses listed in the Microsoft Outlook address book of the infected machine. The subject of the e-mail contains various subjects and "Free Gift" Requested For: <Recipient>. It concludes the message with the following:

- Have fun with your free gift!
- Attachment: Free_Gift.scr

WORM_FREGIT.C (Internet Worm): This worm uses Mail Application Program Interface (MAPI) to send e-mail messages to all addresses listed in the Outlook Address Book of the infected system. The details of the e-mail are as follows:

- Subject: None
- Attachment: SCR file with random filename.

The worm also drops a JavaScript component, JS_FREGIT.C. The dropped JavaScript file also uses MAPI to send e-mail messages. The worm and the JavaScript do not have destructive payloads.

WORM_HOBO.A (Aliases: W32.Hobo@mm, Win32.Hobex worm, Win32/Hobo.A.Worm, W32/Hobo-A, Win32/Hobo.A@mm, I-Worm.Hobex, W32/Hobo@MM) (Internet Worm): This UPX-compressed worm drops files in the Windows directory. It modifies system settings so that a copy of the worm is sent out every time the infected user sends an e-mail with a zipped file attachment (i.e. files with ZIP extension names). Instead of the intended attachment, a copy of the worm is sent out to the e-mail recipient. It leaves the unsuspecting user unaware of the file replacement by retaining the file name of the originally intended attachment. The format of the e-mail message that this worm sends out can be as follows:

- Subject: Emailing: <UserFilename1.zip>; <UserFilename2.zip>; <etc>;
- Message Body: <either empty or contains user data>
- Attachment: <UserFilename1.zip, UserFilename2.zip, etc>

Note that the contents of the subject and message body may vary because the user may modify the said fields before the e-mail is actually sent.

X97M/Yawn.n@MM (Excel 97 Macro Virus): The virus will disable Tools/Macro and Tools/Options from the menu. It will also drop VBS/Cybarm.a as C:\WINDOWS\kernel.exe.vbs. It uses Outlook to send e-mail out to first 50 recipients in AddressList with the following information:

- Subject: Penting !! dari [username]
- Body: di bawah ini laporan yang anda perlukan dalam attachment Excel
- Attachment: Infected excel file

The virus will also make a copy of itself as c:\army.xls and then make a copy of this file in the XLStart directory as: [day] + "S" + [month] + "o".xls. An example of a filename it may create depending on the day and month would be: 27S11o.xls. Due to an error in code, these excel files may not be infected.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AIM-Flood	N/A	CyberNotes-2002-16
Backdoor.AIMVision	N/A	CyberNotes-2002-21
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.AntiLam.20	20	CyberNotes-2002-18
Backdoor.Antilam.g1	g1	CyberNotes-2002-23
Backdoor.Armageddon.B	N/A	CyberNotes-2002-20
Backdoor.Asniffer	N/A	CyberNotes-2002-21
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Assasin.B	B	CyberNotes-2002-23
Backdoor.Assasin.C	**C**	**Current Issue**
Backdoor.Baste	N/A	CyberNotes-2002-23
Backdoor.Bofishy.C	C	CyberNotes-2002-23
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	N/A	CyberNotes-2002-18
Backdoor.Cigivip	N/A	CyberNotes-2002-23
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	N/A	CyberNotes-2002-18
Backdoor.DarkFtp	N/A	CyberNotes-2002-19
Backdoor.DarkSky.B	B	CyberNotes-2002-20
Backdoor.DarkSky.C	C	CyberNotes-2002-21
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Delf.D	D	CyberNotes-2002-22
Backdoor.Delf.E	**E**	**Current Issue**
Backdoor.Dindang	N/A	CyberNotes-2002-22
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.Elitem	N/A	CyberNotes-2002-20
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	N/A	CyberNotes-2002-18
Backdoor.Feardoor	N/A	CyberNotes-2002-21
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Ana	N/A	CyberNotes-2002-20
Backdoor.FTP_Ana.B	B	CyberNotes-2002-20
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.Fulamer.25	**N/A**	**Current Issue**
Backdoor.FunFactory	N/A	CyberNotes-2002-19

Trojan	Version	CyberNotes Issue #
Backdoor.GF.13	N/A	CyberNotes-2002-23
Backdoor.Goster	N/A	CyberNotes-2002-20
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.GWGhost	N/A	CyberNotes-2002-21
Backdoor.Helios	N/A	CyberNotes-2002-19
Backdoor.Hupigeon	N/A	CyberNotes-2002-21
Backdoor.IrcContact	**N/A**	**Current Issue**
Backdoor.Kaitex.B	B	CyberNotes-2002-20
Backdoor.Kaitex.C	C	CyberNotes-2002-22
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Klb	N/A	CyberNotes-2002-22
Backdoor.Kryost	N/A	CyberNotes-2002-18
Backdoor.Lanfilt	**N/A**	**Current Issue**
Backdoor.Laphex	N/A	CyberNotes-2002-18
Backdoor.Laphex.Client	N/A	CyberNotes-2002-18
Backdoor.Lastdoor	N/A	CyberNotes-2002-18
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	B	CyberNotes-2002-18
Backdoor.Litmus.203.b	B	CyberNotes-2002-22
Backdoor.Litmus.2a	2a	CyberNotes-2002-20
Backdoor.LittleWitch.B	B	CyberNotes-2002-22
Backdoor.Malpayo	**N/A**	**Current Issue**
Backdoor.Miffice	N/A	CyberNotes-2002-18
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.Mite	N/A	CyberNotes-2002-18
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.Neodurk	N/A	CyberNotes-2002-23
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.Niovadoor	N/A	CyberNotes-2002-22
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.Optix.04	04	CyberNotes-2002-19
Backdoor.Optix.04.b	B	CyberNotes-2002-22
Backdoor.Optix.04.c	C	CyberNotes-2002-22
Backdoor.OptixPro.10	10	CyberNotes-2002-18
Backdoor.OptixPro.11	11	CyberNotes-2002-20
Backdoor.OptixPro.11.b	B	CyberNotes-2002-22
Backdoor.OptixPro.12	12	CyberNotes-2002-18
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Pest.Cli	N/A	CyberNotes-2002-20
Backdoor.Pestdoor	N/A	CyberNotes-2002-20
Backdoor.Phoenix	N/A	CyberNotes-2002-19
Backdoor.Platrash	N/A	CyberNotes-2002-21
Backdoor.Ptakks.B	N/A	CyberNotes-2002-18
Backdoor.RCServ	N/A	CyberNotes-2002-19
Backdoor.RemoteNC	N/A	CyberNotes-2002-09

Trojan	Version	CyberNotes Issue #
Backdoor.RemoteNC.B	**B**	**Current Issue**
Backdoor.Revrs	N/A	CyberNotes-2002-22
Backdoor.Ripjac	**N/A**	**Current Issue**
Backdoor.RMFDoor.Cli	N/A	CyberNotes-2002-20
Backdoor.Robi	N/A	CyberNotes-2002-18
Backdoor.Roxrat.10	N/A	CyberNotes-2002-20
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Sdbot.B	B	CyberNotes-2002-22
Backdoor.Seamy	N/A	CyberNotes-2002-18
Backdoor.Singu	N/A	CyberNotes-2002-22
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Sparta.B	B	CyberNotes-2002-19
Backdoor.Sparta.C	C	CyberNotes-2002-21
Backdoor.Spigot.B	B	CyberNotes-2002-22
Backdoor.Spoofbot	**N/A**	**Current Issue**
Backdoor.Synrg	N/A	CyberNotes-2002-22
Backdoor.Tela	N/A	CyberNotes-2002-17
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Theef.B	B	CyberNotes-2002-21
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Wiween	N/A	CyberNotes-2002-22
Backdoor.Wold	N/A	CyberNotes-2002-22
Backdoor.Y3KRat.14	**N/A**	**Current Issue**
Backdoor.Y3KRat.15	N/A	CyberNotes-2002-17
Backdoor.Zenmaster	N/A	CyberNotes-2002-19
Backdoor-AKO	N/A	CyberNotes-2002-20
BackDoor-AKR	N/A	CyberNotes-2002-19
BackDoor-ALT	N/A	CyberNotes-2002-21
BackDoor-AMB	N/A	CyberNotes-2002-22
BackDoor-AMH	N/A	CyberNotes-2002-23
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/EHKSLogger	N/A	CyberNotes-2002-19
BDS/Pestdoor.4	N/A	CyberNotes-2002-20
BDS/Sporkbot	N/A	CyberNotes-2002-20
BDS/WinSpyer	N/A	CyberNotes-2002-22
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
Bneo.Trojan	N/A	CyberNotes-2002-18
Cardst	N/A	CyberNotes-2002-17
Cytron	N/A	CyberNotes-2002-20
Diskfill-F	F	CyberNotes-2002-23
Downloader.BO.dr	**dr**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Downloader-BO.b	b	CyberNotes-2002-23
FakeGina.Trojan	N/A	CyberNotes-2002-16
Fortnight	N/A	CyberNotes-2002-10
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
Jekord	N/A	CyberNotes-2002-19
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
Netbus.160.Dropper	N/A	CyberNotes-2002-17
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNCrack	N/A	CyberNotes-2002-18
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16
PWSteal.Antigen	N/A	CyberNotes-2002-23
PWSteal.Avisa	**N/A**	**Current Issue**
PWSteal.BStroj	N/A	CyberNotes-2002-20
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17
PWSteal.SoapSpy	N/A	CyberNotes-2002-18
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
QDel297	N/A	CyberNotes-2002-23
QDel350	**N/A**	**Current Issue**
RCServ	N/A	CyberNotes-2002-10
Reboot-R	N/A	CyberNotes-2002-18
StartPage-B	N/A	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/EvilDX	N/A	CyberNotes-2002-19
Tr/FakeYahoMe	N/A	CyberNotes-2002-23
Tr/Mastaz	N/A	CyberNotes-2002-23
Tr/SCKeyLog.Spy.20	N/A	CyberNotes-2002-22
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/WLoader	N/A	CyberNotes-2002-20
TR/Zirko	N/A	CyberNotes-2002-10
Trj/GhostGirl	N/A	CyberNotes-2002-19
Troj/Apher-A	N/A	CyberNotes-2002-17
Troj/Bdoor-AML	N/A	CyberNotes-2002-23
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/FireAnv-A	N/A	CyberNotes-2002-19
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Netdex-A	N/A	CyberNotes-2002-21
Troj/Nethief-C	N/A	CyberNotes-2002-22
Troj/Ritter-A	N/A	CyberNotes-2002-17
Troj/Tobizan-A	N/A	CyberNotes-2002-16

Trojan	Version	CyberNotes Issue #
Troj/Unreal-A	N/A	CyberNotes-2002-16
Troj/Zasil-A	N/A	CyberNotes-2002-23
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_INOR.A	A	CyberNotes-2002-23
TROJ_INOR.B	B	CyberNotes-2002-23
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMBNUKE.A	N/A	CyberNotes-2002-18
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_SUOMIA.A	N/A	CyberNotes-2002-18
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Adclicker	N/A	CyberNotes-2002-19
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Ahero	**N/A**	**Current Issue**
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.AntiUpdater	N/A	CyberNotes-2002-23
Trojan.Avid	N/A	CyberNotes-2002-19
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	N/A	CyberNotes-2002-18
Trojan.Diskfil	N/A	CyberNotes-2002-19
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Houpe	N/A	CyberNotes-2002-23
Trojan.Iblis	N/A	CyberNotes-2002-22
Trojan.IrcBounce	N/A	CyberNotes-2002-19
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Lovead	N/A	CyberNotes-2002-19
Trojan.Nullbot	N/A	CyberNotes-2002-19
Trojan.Portacopo:br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.Ajim_bbs	N/A	CyberNotes-2002-19
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.PWS.QQPass.C	N/A	CyberNotes-2002-21
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.Win32.Filecoder	N/A	CyberNotes-2002-18
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
Trojan.WinReboot	N/A	CyberNotes-2002-20
UNIX_ALUTAPS.A	N/A	CyberNotes-2002-21
VBS.AVFake	N/A	CyberNotes-2002-22
VBS.Krim.C	N/A	CyberNotes-2002-22
VBS.Lavra.B.Worm	N/A	CyberNotes-2002-19
VBS.Zevach	N/A	CyberNotes-2002-15
VBS/Helvis	N/A	CyberNotes-2002-22
W32.Azak	N/A	CyberNotes-2002-16
W32.Balick.Trojan	**N/A**	**Current Issue**
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15

Trojan	Version	CyberNotes Issue #
W32.Darkgoose.Trojan	**N/A**	**Current Issue**
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16
W32.Kotef	N/A	CyberNotes-2002-16
W32.Libi	N/A	CyberNotes-2002-10
W32.Manifest.Trojan	**N/A**	**Current Issue**
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.STD.D	N/A	CyberNotes-2002-22
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15
Worm/Garra	N/A	CyberNotes-2002-20

Backdoor.Assasin.C (Aliases: Backdoor.Assasin.11, Backdoor-AGS): This is a Backdoor Trojan that gives a malicious user unauthorized access to a compromised computer. Backdoor.Assasin.C is packed using UPX v1.20 and is a variant of Backdoor.Assasin. When Backdoor.Assasin.C runs, it displays this message: "Invalid Jpeg Image," and then copies itself as %windir%\Ms Spool32. Next it creates the %windir%\Ms spool32.dat file. The Trojan creates the value, "Ms Spool32 %windir%\ms spool32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. Also, it creates the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\AUFOBK
- HKEY_LOCAL_MACHINE\SOFTWARE\AUFOBK\eu%t{efn74+fzb

It attempts to disable some antivirus and firewall programs by terminating the active processes. The Trojan notifies the client side using ICQ pager and/or e-mail. Once installed, Backdoor.Assasin.C waits for commands from the remote client.

Backdoor.Delf.E: This is a backdoor Trojan that allows unauthorized access to the computer by opening a port. When Backdoor.Delf.E is executed, it will attempt to copy itself as %windir%\Winallap.exe and %system%\winallapu.exe. Next, the Trojan attempts to add the value, "winallap %windir%\winallap.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

and the value, "winallapu %system%\winallapu.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

As a result, Backdoor.Delf.E runs each time that you start Windows. Each time that Backdoor.Delf.E is executed, it swaps the registry values that it added. For example, if it added winallap %windir%\winallap.exe to:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

the last time that it ran, when you next restart the computer, it removes that value and adds winallapu %system%\winallapu.exe to:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce.

When Backdoor.Delf.E is active in memory, it listens on port 13401 for incoming connections. It has the ability to post messages to a certain newsgroup. It attempts to find the news server for the domain that the infected computer is on, and then contact it. It then attempts to find a message in the newsgroup and reply to it.

Backdoor.Fulamer.25: This is a typical backdoor Trojan which gives remote malicious users unobstructed access to your computer. It is written in the Borland Delphi programming language. When Backdoor.Fulamer.25 runs, it copies itself to the %system% folder. It opens two TCP ports to connect to the malicious user. The exact file names and port numbers that it uses may vary from version to version, because the malicious user who creates this Backdoor Trojan can choose any desired file name. It adds a value that refers to the dropped Trojan file to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you restart Windows. For example, if the file that the Trojan dropped was System.exe, it would add the value, System C:\%system%\system.exe, to the previously mentioned key. When the malicious user creates the Backdoor.Fulamer.25 server file, there are many functions that can be added.

Backdoor.IrcContact (Alias: Backdoor.IrcContact.20): This is a backdoor Trojan that gives a malicious user unauthorized access to an infected computer. By default it opens port 6667 on the infected computer. Backdoor.IrcContact is packed using ASPack v2.12. When Backdoor.IrcContact runs, it copies itself as Syswin32.exe or Syswin.exe into the %system% folder. In addition, it drops the file Syswin32.dll or Syswin.dll (this is a text file that contains the Trojan's connection settings) into the %system% folder. The Trojan creates one of these values:

- syswin32   %system%\syswin32.exe
- syswin   %system%\syswin.exe

in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process, so that it continues to run after you log off. In this case, Backdoor.IrcContact closes only when the system is shut down. After Backdoor.IrcContact is installed, it joins a specific IRC channel and then waits for commands from the remote client.

Backdoor.Lanfilt: This is a backdoor Trojan that allows a malicious user to gain access to the computer. The malicious user can then delete, copy, and execute files and perform other actions. When Backdoor.Lanfilt runs, it copies itself as C:\%windir%\Run322.exe and adds the value, “System C:\%windir%\run322.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It creates a log file named C:\001.sys. The Trojan opens three TCP ports to allow the malicious user to remotely control the infected computer. It attempts to terminate the process of security software, such as antivirus, firewall, and system-monitoring programs.

Backdoor.Malpayo: This backdoor Trojan allows a malicious user to remotely control an infected computer. It is written in the Borland Delphi programming language and compressed with UPX. When Backdoor.Malpayo runs, it copies itself as C:\Windows\System32\Sys.exe and adds the value, “System C:\Windows\System32\Sys.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you restart Windows. It creates the subkey winzip to the registry key:

- HKEY_LOCAL_MACHINE\Software

Once installed, Backdoor.Malpayo waits for commands from the remote client.

Backdoor.RemoteNC.B: This is a backdoor Trojan that allows a malicious user to gain access to your system. The malicious user can then delete, copy, and execute files and perform other actions. By default it opens port 19340.

Backdoor.Ripjac (Alias: Backdoor-ANK): This is a backdoor Trojan that allows a malicious user to gain access to the infected computer. The presence of the file Synchost.exe is an indication of a possible infection. When Backdoor.Ripjac runs, it copies itself as C:\%windir%\Synchost.exe and adds the value, “Remote Access Slave C:\%windir%\Synchost.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. By default, the Trojan opens port 4999 to allow the malicious user to remotely control the infected computer

Backdoor.Spoofbot: This is a malicious backdoor program that allows a remote malicious user to perform harmful activities such as SYN and UDP flooding. When Backdoor.Spoofbot runs, it opens a TCP and a UDP port and listens on that port for a few seconds. If no connection is made, Backdoor.Spoofbot closes the port and selects another port for listening. The port number selection is in an increasing sequence, although the increments are randomly selected. Backdoor.Spoofbot acts as a "knight" that performs specific activities as instructed by the malicious user.

Backdoor.Y3KRat.14 (Aliases: Backdoor.Y3KRat.14.b, BackDoor-GQ.svr, BKDR_Y3KRAT.14.A): This is a backdoor Trojan that gives a malicious user unauthorized access to an infected computer. It makes use of ports 5882, 5884, 5888, and 5889 and attempts to obtain system passwords. It is a Delphi application, and it is packed with UPX v1.02. Backdoor.Y3KRat.14 is a variant of Backdoor.Y3KRat.12. When Backdoor.Y3KRat.14 runs, it copies itself as C:\Windows\Messenger.exe and creates the value, "Yahoo! C:\Windows\Yahoo!Messenger.exe," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start or restart Windows. The Trojan registers itself as a service process, so that it continues to run after you log off. In this case, Backdoor.Y3KRat.14 closes only when you shut down the computer. In addition, Backdoor.Y3KRat.14 attempts to obtain access to the password cache that is stored on the local computer. The cached passwords include modem and dial-up passwords, URL passwords, share passwords, and others. The Trojan uses ICQ pager to notify the client side. After Backdoor.Y3KRat.14 is installed, it waits for commands from the remote client.

Downloader.BO.dr: This is a Trojan that drops Downloader.BO onto the infected system. Several variants have been found. They are all .html files. Downloader.BO.dr arrives disguised as an administrative e-mail that may have the following characteristics:

- From: MAILER-DAEMON@<recipient domain>
- Subject: FAILED DELIVERY
- Attachment: Mail.hta

If you open the attachment, it displays this fake advertisement. It copies one of these files to your computer, both of which are Downloader.BO Trojan, and then executes it:

- C:\Sys615.scr
- C:\Progra~1\Outloo~1\outl32.scr

PWSteal.Avisa (Alias: Trojan.PSW.Avisa): This is a password-stealing Trojan. It is written in Microsoft Visual Basic version 6. When it is executed, it drops the file %windir%\Test de inteligencia.html and opens it with your Web browser. Test de inteligencia.html is written in Spanish and it indicates that it is a test. It is not malicious and as such. The Trojan then copies itself as %system%\RundII32.exe and creates the value, "RunDII32 %sysdir%\RundII32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. The Trojan attempts to send steal information by using FTP commands.

QDel350 (Alias: Trj/Balleig): This Trojan attempts to delete all files on the C: driver. It is written in Visual Basic 6 and therefore requires the VB 6 runtime library files in order to run. This is a common programming language; therefore most users will have the required files to run the Trojan. However, the file deletion payload will not function on Windows 9x/ME. When run, the Trojan creates a batch file on the root of the C:\ drive, Abracadabra.bat. This batch file contains instructions to delete all files in the following directories and subdirectories:

- C:\*.*
- C:\windows\*.*
- C:\windows\system\*.*
- C:\windows\system32\*.*

Several message boxes are displayed in succession. After the last "OK" is pressed, the batch file is then run. However, due to the command line parameters used by the Trojan, it will only run on NT based systems.

Trojan.Ahero: This is a Trojan horse that is written in Visual Basic. It will delete the file Msconfig.exe and attempts to delete the file Install.exe file from the root folder of some local drives. When Trojan.Ahero runs, it copies itself as %system%\Ntvbm.exe and runs as a service. If the file name that the Trojan creates is not Ntvbm.exe, the Trojan deletes itself. This Trojan adds the value, "ntvbm ntvbm.exe," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows. Trojan.Ahero also deletes Msconfig.exe, and then it copies the Kernel32.dll file--using the file name the Msconfig.exe--from the %system% folder to the folder that contained the deleted Msconfig.exe file.

W32.Balick.Trojan: This is a Trojan horse that attempts to obtain an ad-click credit for the Trojan's author. It will copy itself to the \System folder as Csss.exe.

W32.Darkgoose.Trojan: This is a Visual Basic application that creates and executes a batch file that will delete all files from C:\, C:\Windows, C:\Windows\System and C:\Windows\System32. When it is executed, W32.Darkgoose.Trojan creates the file C:\Abracadabra.bat. This batch file contains instructions to delete all files from these folders:

- C:\
- C:\Windows
- C:\Windows\System
- C:\Windows\System32

The paths are hardcoded within the Trojan. The Trojan then displays a series of dialog boxes. After displaying the last line, W32.Darkgoose.Trojan executes the batch file in a hidden window. It waits for it to finish and then deletes it.

W32.Manifest.Trojan: This is a Trojan horse that installs an ftp server, a monitoring program, and a mail server on the infected computer. W32.Manifest.Trojan is currently being distributed through the KaZaA file-sharing network as a XVID codec.